The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

12/05/2014

SUBJECT:

Multiple Vulnerabilities in WordPress Download Manager Plugin Could Allow Remote Code Execution

EXECUTIVE SUMMARY:

Multiple vulnerabilities in the WordPress Download Manager plugin may allow remote code execution. WordPress Download Manager is a file and document management plugin for the WordPress content management system.

Successful exploitation could result in an attacker compromising data security, potentially allowing access to confidential data, or could compromise processing resources in a user's computer.

SYSTEM AFFECTED:

- WordPress Download Manager Plugin. Versions prior to 2.7.5 are vulnerable.

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

WordPress Download Manager is prone to multiple vulnerabilities including one that could allow for remote code execution due to a failure to sanitize user-supplied input submitted to the ‘execute’ parameter of the 'wpdm_ajax_call_exec()' function. A remote file-include vulnerability also exists because it allows the uploading of arbitrary files to the '/file-type-icons/' directory. Specifically, this issue affects the 'wpdm_upload_icon()' function.

Successful exploitation of these vulnerabilities could result in an attacker being able to execute arbitrary code in the context of the web server process or could allow for the uploading of arbitrary files. This may allow an attacker access to sensitive information and compromise the application.

RECOMMENDATIONS:

The following actions should be taken:

- If using the plugin, update to its most current version, 2.7.5.
- Review and follow WordPress hardening guidelines - http://codex.wordpress.org/Hardening_WordPress
- Confirm that the operating system and all other applications on the system running this CMS are updated with the most recent patches.
- Deploy NIDS to detect and block attacks and anomalous activity such as crafted requests containing suspicious URI sequences.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Security Focus:

http://www.securityfocus.com/bid/71490